Steane-enlargement of quantum codes from the Hermitian function field

Christensen, René Bødker; Geil, Olav

Published in:
Designs, Codes and Cryptography

DOI (link to publication from Publisher):
10.1007/s10623-019-00709-7

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

Steane-Enlargement of Quantum Codes from the Hermitian Function Field

René Bødker Christensen and Olav Geil

Department of Mathematical Sciences, Aalborg University, Denmark.
{rene,olav}@math.aau.dk

Abstract

In this paper, we study the construction of quantum codes by applying Steane-enlargement to codes from the Hermitian function field. We cover Steane-enlargement of both usual one-point Hermitian codes and of order bound improved Hermitian codes. In particular, the paper contains two constructions of quantum codes whose parameters are described by explicit formulae, and we show that these codes compare favourably to existing, comparable constructions in the literature. Furthermore, a number of the new codes meet or even exceed the quantum Gilbert-Varshamov bound.

Keywords: Algebraic geometric code, Quantum code, Steane-enlargement, Hermitian function field

2000 MSC: 94B27, 81Q99

1 Introduction

The prospect of quantum computers potentially surpassing the computational abilities of classical computers has spawned much interest in studying and building large-scale quantum computers. Since such quantum systems would be very susceptible to disturbances from the environment and to imperfections in the quantum gates acting on the system, the implementation of a working quantum computer requires some form of error-correction. This has led to the study of quantum error-correcting codes, and although such codes are conceptually similar to their classical brethren, their construction calls for different techniques. Nevertheless, results have been found that link classical codes to quantum ones, suggesting that good quantum codes may be found by considering good classical codes.

A well-known class of algebraic geometric codes is the one-point codes from the Hermitian function field. For these one-point Hermitian codes, one of the simplest bounds on the minimal distance is the Goppa bound. For codes of sufficiently large dimension, however, the Goppa bound does not give the true minimal distance, and the order bound for dual codes [5, 12] and for primary codes [1, 9, 10] give more information on the minimal

This is a post-peer-review, pre-copyedit version of an article published in *Designs, Codes and Cryptography*. The final authenticated version is available online at: https://doi.org/10.1007/s10623-019-00709-7

distance of the codes. These improved bounds also give rise to a family of improved codes with designed minimal distances, and we shall refer to such codes as *order bound improved* codes.

The construction of quantum codes from one-point Hermitian codes has already been considered in [21], and from order bound improved Hermitian codes in [3]. Neither of these works, however, explore the potential benefit from applying Steane-enlargement to the codes under consideration. Thus, this paper will address this question, and describe the quantum codes that can be obtained in this manner.

The work is structured as follows. Section 2 contains the preliminary theory on quantum codes and order bound improved Hermitian codes that will be necessary in the subsequent sections. Afterwards, Section 3 covers the results of applying Steane-enlargement to one-point Hermitian codes and order bound improved Hermitian codes. The parameters of the resulting codes are then compared to codes already in the literature and to the quantum Gilbert-Varshamov bound in Section 4. Section 5 contains the concluding remarks.

2 Preliminaries

In this section, we shall reiterate the necessary definitions and results regarding both quantum error-correcting codes and order bound improved Hermitian codes. For both of these, we will be relying on nested pairs of classical codes, and on the relative distance of such pairs. Thus, recall that for classical, linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$, we define the relative distance of the pair as

$$d(\mathcal{C}_1, \mathcal{C}_2) = \min\{w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1 \setminus \mathcal{C}_2\},$$

where w_H denotes the Hamming weight.

Quantum codes

A k-dimensional quantum code of length n over $\mathbb{F}_q$ is a q^k-dimensional subspace of the Hilbert space $\mathbb{C}^{q^n}$. This space is subject to phase-shift errors, bit-flip errors, and combinations thereof. For a quantum code, we define its two minimal distances d_z and d_x as the maximal integers such that the code allows simultaneous detection of any $d_z - 1$ phase-shift errors and any $d_x - 1$ bit-flip errors. When such a code has length n and dimension k, we refer to it as an $[[n, k, d_z/d_x]]_q$-quantum code.

The literature contains many works based on the assumption that it is not necessary to distinguish between the two types of errors. Thus, the quantum code is only associated with a single minimal distance. That is, we say that its minimal distance is $d = \min\{d_z, d_x\}$, and the notation for the parameters is presented slightly more compactly as $[[n, k, d]]_q$. In this case, we refer to the quantum code as being *symmetric*, and in the previous case we refer to it as being *asymmetric*.

One of the commonly used constructions of quantum codes was provided by Calderbank, Shor, and Steane [2, 22] and relies on a dual-containing, classical error-correcting code in order to obtain a quantum stabilizer code. That is, it relies on a classical code $\mathcal{C}$ which contains its Euclidean dual $\mathcal{C}^\perp$. It was later shown that the dual-containing code can be replaced by a pair of nested codes, giving asymmetric quantum codes. This generalized CSS-construction is captured in the following theorem found in [20].

Theorem 1. *Given $\mathbb{F}_q$-linear codes $\mathcal{C}_2 \subsetneq \mathcal{C}_1$ of length n and codimension ℓ, the CSS-construction ensures the existence of an asymmetric quantum code with parameters*

$$[[n, \ell, d_z/d_x]]_q$$

where $d_z = d(\mathcal{C}_1, \mathcal{C}_2)$ and $d_x = d(\mathcal{C}_2^\perp, \mathcal{C}_1^\perp)$.

Corollary 2. *If the $[n, k, d]$ linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is dual-containing, then a*

$$[[n, 2k - n, d]]_q$$

symmetric quantum code exists.

When the CSS-construction is applied to a dual-containing binary linear code as in Corollary 2, Steane [23] proposed a procedure whereby the dimension of the resulting quantum code may be increased. In the best case, this can be done with little or no decrease in the minimal distance of the quantum code. This procedure – eponymously named Steane-enlargement in the literature – has later been generalized to q-ary codes as well [11, 17].

Theorem 3. *Consider a linear $[n, k]$ code $\mathcal{C} \subseteq \mathbb{F}_q^n$ that contains its Euclidean dual $\mathcal{C}^\perp$. If $\mathcal{C}'$ is an $[n, k']$ code such that $\mathcal{C} \subsetneq \mathcal{C}'$ and $k' \geq k + 2$, then an*

$$\left[\left[n, k + k' - n, \geq \min\left\{d, \left\lceil (1 + \tfrac{1}{q})d' \right\rceil\right\}\right]\right]_q$$

quantum code exists with $d = d(\mathcal{C}, \mathcal{C}'^\perp)$ and $d' = d(\mathcal{C}', \mathcal{C}'^\perp)$.

When presenting the parameters of a Steane-enlarged code in propositions of this paper, we will often state the dimension in the form $2k - n + (k' - k)$. In this way, we highlight the dimension increase since $2k - n$ is the dimension of the non-enlarged quantum code.

Order bound improved Hermitian codes

We first recall a number of definitions regarding the Hermitian function field. For more details, the reader is referred to [24]. The Hermitian function field $\mathbb{H}$ over $\mathbb{F}_{q^2}$ is the function field $\mathbb{F}_{q^2}(X, Y)$ defined by the equation $X^{q+1} = Y^q + Y$. It is well-known that $\mathbb{H}$ has $q^3 + 1$ rational places, which we will denote by $P_1, P_2, \ldots, P_{q^3}, Q$ where Q is the unique common pole of X and Y. A divisor of a function field is a formal sum of places, and for the purpose of coding theory the divisor $D = P_1 + P_2 + \cdots + P_n$ where $n = q^3$ is commonly used.

For any integer λ, the Riemann-Roch space

$$\mathcal{L}(\lambda Q) = \{f \in \mathbb{H} \mid (f) \geq -\lambda Q\} \cup \{0\}$$

contains – in addition to zero – all the elements of $\mathbb{H}$ that have pole order at most λ in Q and no other poles. Here, (f) is the principal divisor of f. The one-point algebraic geometric code associated with the divisors D and λQ is then

$$C_{\mathcal{L}}(D, \lambda Q) = \{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in \mathcal{L}(\lambda Q)\},$$

where $f(P_i)$ denotes the residue class map. Since the support of D contains only rational places and none of these are Q, it may be shown that $C_{\mathcal{L}}(D, \lambda Q) \subseteq \mathbb{F}_{q^2}^n$ and that it is indeed a linear code.

The codes defined below rely heavily on the Weierstraß semigroup of Q. We denote this by $H(Q)$, and it contains the non-negative integers λ such that $-\nu_Q(f) = \lambda$ for some $f \in \bigcup_{i=0}^{\infty} \mathcal{L}(iQ)$. As in [3, 10], we consider a special subset of $H(Q)$, namely

$$H^*(Q) = \{\lambda \in H(Q) \mid C_{\mathcal{L}}(D, \lambda Q) \neq C_{\mathcal{L}}(D, (\lambda - 1)Q)\}.$$

It may be shown that in fact

$$H^*(Q) = \{iq + j(q+1) \mid 0 \leq i < q^2,\ 0 \leq j < q\}. \tag{1}$$

Now, fix an element $f_\lambda \in \mathcal{L}(\lambda Q) \setminus \mathcal{L}((\lambda - 1)Q)$ for each $\lambda \in H^*(Q)$, and define the map $\sigma\colon H^*(Q) \to \mathbb{N}$ given by

$$\sigma(iq + j(q+1)) = \begin{cases} q^3 - iq - j(q+1) & \text{if } 0 \leq i < q^2 - q \\ (q^2 - i)(q - j) & \text{if } q^2 - q \leq i < q^2 \end{cases}. \tag{2}$$

This map is the order bound for primary Hermitian codes, and it provides a lower bound on the weight of codewords. In particular, any codeword in $C_{\mathcal{L}}(D, \lambda Q) \setminus C_{\mathcal{L}}(D, (\lambda - 1)Q)$ has weight at least $\sigma(\lambda)$. Thus, by strategically picking out only those codewords that are guaranteed to have a certain designed distance, it is possible to construct an improved primary code

$$\tilde{E}(\delta) = \mathrm{Span}_{\mathbb{F}_{q^2}}\{(f_\lambda(P_1), f_\lambda(P_2), \ldots, f_\lambda(P_n)) \mid \sigma(\lambda) \geq \delta\}.$$

Furthermore, it was shown in [3] as a special case of [9] that $\tilde{E}(\delta)$ has minimal distance exactly δ whenever $\delta \in \sigma(H^*(Q))$.

For the order bound to produce an improved code, the designed distance must be sufficiently small. Otherwise, the code $\tilde{E}(\delta)$ simply corresponds to one of the usual one-point Hermitian codes. This correspondence is given in the following result from [3; Cor. 4].

Lemma 4. *For $\delta > q^2 - q$ we have $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, but $C_{\mathcal{L}}(D, (q^3 - (q^2 - q))Q)$ is strictly contained in $\tilde{E}(q^2 - q)$.*

For $\delta \leq q^2 - q$, the work [3] contains a lower bound on the dimension of $\tilde{E}(\delta)$. In Proposition 6 below, we give an explicit formula describing the dimension in this case. This formula relies on the number of (number theoretic) divisors of a certain type, as specified in the following definition.

Definition 5. *For $n \in \mathbb{Z}_+$, we let $\tau^{(q)}(n)$ denote the number of divisors d of n such that $0 \leq d \leq q$ and $n/d \leq q$.*

From the definition it should be clear that $\tau^{(q)}(n)$ can be computed in $\mathcal{O}(q)$ operations.

Proposition 6. *Let $1 \leq \delta \leq q^2$, and write $\delta - 1 = aq + b$ for $0 \leq b < q$. Then*

$$\dim(\tilde{E}(\delta)) = q^3 - q^2 - \frac{a(a-1)}{2} - \min\{a, b\} + \sum_{i=\delta}^{q^2} \tau^{(q)}(i).$$

Proof. We give the proof by partitioning $H^*(Q)$ in three disjoint sets:

$$\begin{aligned}
\Lambda_1 &= \{iq + j(q+1) \in H^*(Q) \mid i + j < q^2 - q,\ 0 \leq i < q^2 - q,\ 0 \leq j < q\} \\
\Lambda_2 &= \{iq + j(q+1) \in H^*(Q) \mid i + j \geq q^2 - q,\ 0 \leq i < q^2 - q,\ 0 \leq j < q\} \\
\Lambda_3 &= \{iq + j(q+1) \in H^*(Q) \mid q^2 - q \leq i < q^2,\ 0 \leq j < q\}.
\end{aligned}$$

We first determine the cardinality of Λ_2. Considering some $iq + j(q+1) \in \Lambda_2$, and writing $i = q^2 - q - k$, there are $q - k$ possible values of j. There are $q - 1$ such integers k since $q^2 - 2q + 1 \leq i < q^2 - q$ within the set Λ_2. This implies that

$$|\Lambda_2| = \sum_{k=1}^{q-1} (q - k) = \frac{q(q-1)}{2} = g,$$

where g is the genus of the Hermitian function field. From this, it is also seen that $|\Lambda_1| = q^3 - q^2 - |\Lambda_2| = q^3 - q^2 - g$.

All elements λ of Λ_1 satisfy $\sigma(\lambda) = q^3 - \lambda$. The largest element λ' in Λ_1 is given by $\lambda' = (q^2 - 2q)q + (q-1)(q+1)$, which has $\sigma(\lambda') = q^2 + 1$. Thus, all elements of Λ_1 have $\sigma(\lambda) \geq \delta$, meaning that Λ_1 contributes $|\Lambda_1| = q^3 - q^2 - g$ to the dimension of $\tilde{E}(\delta)$.

In order to determine the number of elements in Λ_2 that satisfy $\sigma(\lambda) \geq \delta$, we compute $|\Lambda_2| - |\{\lambda \in \Lambda_2 \mid \sigma(\lambda) < \delta\}|$. As was the case for Λ_1, all elements of Λ_2 have $\sigma(\lambda) = q^3 - \lambda$. From this it follows that

$$\sigma(\Lambda_2) = \{q+1, 2q+1, 2q+2, 3q+1, 3q+2, 3q+3, 4q+1, \ldots, (q-1)q+(q-1)\}.$$

Combining this with the assumption that $\delta - 1 = aq + b$, where both a and b are non-negative, the number of elements in $\sigma(\Lambda_2)$ smaller than δ is exactly

$$\sum_{i=1}^{a-1} i + \min\{a, b\} = \frac{a(a-1)}{2} + \min\{a, b\}.$$

Because the total number of elements is $|\Lambda_2| = g$, the set Λ_2 contributes $g - a(a-1)/2 - \min\{a, b\}$ to the dimension.

Finally, consider $\sigma(\Lambda_3) = \{\sigma(\lambda) \mid \lambda \in \Lambda_3\}$ as a multiset. We will count (with multiplicity) the number of elements $s \in \sigma(\Lambda_3)$ with $s \geq \delta$. Observe that $\sigma(\lambda) = (q^2 - i)(q - j)$ for all the elements $\lambda = iq + j(q+1) \in \Lambda_3$. Hence, $s \in \sigma(\Lambda_3)$, if and only if $s = d \cdot \frac{s}{d}$ where $d \leq q$ and $\frac{s}{d} \leq q$. Since there are $\tau^{(q)}(s)$ such divisors d, it follows that the multiplicity of s in $\sigma(\Lambda_3)$ is given by $\tau^{(q)}(s)$. Subsequently, the number of elements satisfying $s \geq \delta$ is

$$\sum_{s=\delta}^{q^2} \tau^{(q)}(s).$$

By summing the contribution from each of the sets Λ_1, Λ_2, and Λ_3, we obtain the dimension as claimed. □

We note that the dimension formula in Proposition 6 does not provide an efficient method for computing the dimension of the code $\tilde{E}(\delta)$. Since the set Λ_3 defined in the proof has q^2 elements, we can loop over all of these and compute the σ-value of each in $\Theta(q^2)$ operations, thus determining the dimension of $\tilde{E}(\delta)$. Using the formula in Proposition 6, however, requires the computation of $\tau^{(q)}(s)$ for up to q^2 values of s. This gives a total complexity of $\mathcal{O}(q^3)$ operations. The formula in Proposition 6 does, however, provide an advantage when we are not interested in a dimension, but rather certain codimensions as will be the case in Section 3. Here, we will only need to compute $\tau^{(q)}$ for m values, where m is a small integer; typically $m = 1$ or $m = 2$.

If only a lower bound for the dimension is needed, Lemma 6 of [3] implies that the sum in Proposition 6 can be bounded below by $q^2 - \lfloor \delta + \delta \ln(q^2/\delta) \rfloor$ for $q \leq \delta < q^2$ and by $q^2 - \lfloor \delta + \delta \ln(\delta) \rfloor$ for $\delta < q$.

3 Steane-enlargement of Hermitian codes

In order to apply Steane-enlargement to the codes defined in Section 2, we now determine a necessary and sufficient condition for $\tilde{E}(\delta)$ to be dual-containing. While this is possible to do by considering the improved codes directly, it is easier to prove via a condition for the usual one-point Hermitian codes to be dual-containing. The latter is well-known, and the following result was given in [25], and can also be found in [24; Prop. 8.3.2].

Proposition 7. *The code $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$ is dual-containing, if and only if*

$$\delta \leq \left\lfloor \frac{1}{2}(q^3 - q^2 + q) \right\rfloor + 1. \tag{3}$$

Corollary 8. *The code $\tilde{E}(\delta)$ is dual-containing, if and only if δ satisfies* (3).

Proof. For $\delta > q^2 - q$, Lemma 4 ensures that $\tilde{E}(\delta) = C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, and the result follows from Proposition 7. For smaller values of δ, the result follows from the observation that $\tilde{E}(q^2 - q + 1) \subsetneq \tilde{E}(\delta)$. □

In Theorem 3, the relative distances $d(\mathcal{C}, \mathcal{C}'^{\perp})$ and $d(\mathcal{C}', \mathcal{C}'^{\perp})$ of the code pairs are used to determine the distance of the resulting quantum code. In the case of one-point Hermitian codes and order bound improved Hermitian codes, however, these specific relative distances coincide with the corresponding non-relative distances. To see this, consider two codes $\mathcal{C}$ and $\mathcal{C}'$ that are either of the form $C_{\mathcal{L}}(D, \lambda Q)$ or $\tilde{E}(\delta)$. In order to apply Theorem 3, we must require $\mathcal{C}^{\perp} \subsetneq \mathcal{C} \subsetneq \mathcal{C}'$, and we claim that this implies $d(\mathcal{C}, \mathcal{C}'^{\perp}) = d(\mathcal{C})$ and $d(\mathcal{C}', \mathcal{C}'^{\perp}) = d(\mathcal{C}')$. Indeed, since $\mathcal{C}$ is dual-containing, Proposition 7 and Corollary 8 ensure that it contains the smallest dual-containing Hermitian code. That is, $C_{\mathcal{L}}(D, (q^3 - \delta_{\max})Q) \subseteq \mathcal{C}$ where $\delta_{\max} = \left\lfloor \frac{1}{2}(q^3 - q^2 + q) \right\rfloor + 1$ as in (3). This observation combined with $\mathcal{C} \subsetneq \mathcal{C}'$ implies the inclusion $\mathcal{C}'^{\perp} \subsetneq C_{\mathcal{L}}(D, (q^3 - \delta_{\max})Q)$, which in turn gives $\mathcal{C}'^{\perp} \subseteq C_{\mathcal{L}}(D, (q^3 - \delta_{\max} - 1)Q)$. Thus, every codeword of $\mathcal{C}'^{\perp}$ has Hamming weight at least $d(C_{\mathcal{L}}(D, (q^3 - \delta_{\max} - 1)Q)) = \delta_{\max} + 1$. This exceeds both $d(\mathcal{C})$ and $d(\mathcal{C}')$, and our claim on the relative distances follows. For this reason, we only need to consider the non-relative distances in the proofs below.

In the following proposition, we explore the Steane-enlargement from Theorem 3 applied to the usual one-point Hermitian codes. That is, we show by how much the dimension of the symmetric quantum error correcting code can be increased without decreasing its minimal distance. Before giving the result itself, we state the following lemma, which follows from [26].

Lemma 9. *Let $g = q(q-1)/2$ be the genus of the Hermitian function field. If $\lambda \in \mathbb{N}$ satisfies $2g \leq \lambda < q^3$, then $\lambda \in H^*(Q)$.*

Proposition 10. *Assume that δ satisfies (3), and additionally that $\delta \geq q^2 + 3$. If k denotes the dimension of $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$, then there exists a quantum code with parameters*

$$\left[\left[q^3, 2k - q^3 + \left\lceil \tfrac{\delta - 1}{q^2 + 1} \right\rceil, \geq \delta\right]\right]_{q^2}. \tag{4}$$

Proof. According to Proposition 7, the code $C_{\mathcal{L}}(D, (q^3 - \delta)Q)$ is dual-containing. Letting $\delta' = \delta - \lceil (\delta - 1)/(q^2 + 1) \rceil$, it is also seen that $C_{\mathcal{L}}(D, (q^3 - \delta)Q) \subseteq C_{\mathcal{L}}(D, (q^3 - \delta')Q)$. Lemma 9 ensures that the $\lceil (\delta - 1)/(q^2 + 1) \rceil$ integers $\delta - 1, \delta - 2, \ldots, \delta'$ are all included in $H^*(Q)$, meaning that the dimension of $C_{\mathcal{L}}(D, (q^3 - \delta')Q)$ is $k + \lceil (\delta - 1)/(q^2 + 1) \rceil \geq k + 2$. Thus, we can apply Theorem 3 to obtain a quantum code over $\mathbb{F}_{q^2}$ of length and dimension as in (4). This code has minimal distance at least δ since

$$\left(1 + \frac{1}{q^2}\right)\delta' > \left(1 + \frac{1}{q^2}\right)\left(\delta - \frac{\delta - 1}{q^2 + 1} - 1\right) = \delta - 1,$$

and since Lemma 4 ensures that $d\big(C_{\mathcal{L}}(D, (q^3 - \delta)Q)\big) = d(\tilde{E}(\delta)) = \delta$. □

We now turn our attention to the order bound improved codes, and begin by considering the case where both codes can be described as improved codes.

Proposition 11. *Assume that $\delta \in \sigma(H^*(Q))$, and that $2 \leq \delta \leq q^2$. Let k denote the dimension of $\tilde{E}(\delta)$, and choose an $m \in \{1, 2, \ldots, \delta - 1\}$. Write $\delta - 1 = aq + b$ and $\delta - m - 1 = a'q + b'$ such that $0 \leq b, b' < q$, and define*

$$K = \min\{a, b\} - \min\{a', b'\} + \frac{a(a-1) - a'(a'-1)}{2} + \sum_{i=1}^{m} \tau^{(q)}(\delta - i). \quad (5)$$

If $K \geq 2$, then there exists a $[[q^3, 2k - q^3 + K, \geq \delta - m + 1]]_{q^2}$ quantum code.

Proof. Consider any m such that $1 \leq m < \delta$, and define $\delta' = \delta - m$. By Corollary 8, the code $\tilde{E}(\delta)$ is dual-containing. Furthermore, $\tilde{E}(\delta) \subsetneq \tilde{E}(\delta')$, and Proposition 6 implies that the dimension difference is $\dim(\tilde{E}(\delta')) - \dim(\tilde{E}(\delta)) = K$. Thus, if $K \geq 2$, we can apply Theorem 3 to obtain a quantum code, whose dimension is $2k - q^3 + K$. To determine its minimal distance, we see that

$$\left\lceil \left(1 + \frac{1}{q^2}\right) \delta' \right\rceil = \left\lceil (\delta - m) + \frac{\delta - m}{q^2} \right\rceil = \delta - m + 1.$$

The result follows from the fact that $\min\{\delta, \delta - m + 1\} = \delta - m + 1$. □

To fully describe the quantum codes that can be constructed using the order bound improved codes, it is also necessary to consider the case where an ordinary one-point Hermitian code is enlarged to an improved code. Otherwise, we would neglect certain cases where the order bound improved codes are in some sense 'too good' to be used for enlargement as shown in the following example.

Example 1. *Consider the code pair $C_{\mathcal{L}}(D, 52Q) \subsetneq C_{\mathcal{L}}(D, 54Q)$ over $\mathbb{F}_{16}$. These codes have codimension 2, and $C_{\mathcal{L}}(D, 52Q)$ is dual-containing, meaning that we can apply Theorem 3 to obtain a quantum code of dimension $2 \cdot 47 - 64 + 2 = 32$ and minimal distance $d = \min\{12, (1 + 1/16) \cdot 10\} = 11$. Using improved codes only, it is not possible to obtain as good parameters. The reason for this is that the codimension between $\tilde{E}(12)$ and $\tilde{E}(10)$ is only 1. In fact, we have the inclusions*

$$C_{\mathcal{L}}(D, 52Q) \subsetneq \tilde{E}(12) \subsetneq \tilde{E}(10) = C_{\mathcal{L}}(D, 54Q).$$

Thus, if we restrict ourselves to improved codes only, we need to either start from a code smaller than $\tilde{E}(12)$ or enlarge to a code larger than $\tilde{E}(10)$. But neither option gives as good parameters as applying Steane-enlargement to $C_{\mathcal{L}}(D, 52Q) \subsetneq \tilde{E}(10)$.

Despite the above observations, we shall refrain from stating the resulting parameters in a separate proposition since it would essentially say no more than Theorem 3. That is, such enlargements are generally not well-behaved enough to give meaningful formulae for their codimensions and minimal distances apart from the obvious ones, which already appear in Theorem 3.

To conclude this section, we give a few examples over $\mathbb{F}_{16}$ to illustrate the constructions presented in this section.

Example 2. *Let $q = 4$, $\delta = 20$, and consider the code $C_{\mathcal{L}}(D, (q^3 - \delta)Q) = C_{\mathcal{L}}(D, 44Q)$. As in Proposition 10 we set $\delta' = 20 - \lceil 19/17 \rceil = 18$, and apply Theorem 3 to the pair $C_{\mathcal{L}}(D, 44Q) \subsetneq C_{\mathcal{L}}(D, 46Q)$. This yields a quantum code with parameters $[[64, 16, 20]]_{16}$. Had we instead applied Corollary 2 directly to $C_{\mathcal{L}}(D, 44Q)$, the resulting parameters would be $[[64, 14, 20]]_{16}$.*

Example 3. *The order bound improved code $\tilde{E}(5)$ is dual-containing by Corollary 8, and has parameters $[64, 56, 5]_{16}$. This code is contained in $\tilde{E}(4)$, which is a $[64, 59, 4]_{16}$-code. By applying the Steane-enlargement-technique, Theorem 3, we obtain a quantum code of length 64, dimension $2 \cdot 56 - 64 + 3$, and a minimal distance of at least*

$$\min\left\{5, \left\lceil \left(1 + \frac{1}{16}\right) 4 \right\rceil\right\} = 5.$$

That is, we can construct a $[[64, 51, 5]]_{16}$-quantum code. If only one-point Hermitian codes are used, the best quantum code of dimension 51 has parameters $[[64, 51, 4]]_{16}$ stemming from $C_{\mathcal{L}}(D, 60Q) \subsetneq C_{\mathcal{L}}(D, 66Q)$.

A graphical representation of the code inclusions can be found in Figure 1. Here, the top grid shows $H^*(Q)$ arranged according to indices i and j as in (1). The bottom grid shows the same arrangement, but with the map σ from (2) applied to each element.

The different shaded regions indicate the basis vectors of the codes $\tilde{E}(5)$, and $\tilde{E}(4)$ used above. The code $\tilde{E}(5)$ is spanned by codewords on the form $(f_\lambda(P_1), f_\lambda(P_2), \ldots, f_\lambda(P_n))$ with $\sigma(\lambda) \geq 5$. The elements $\lambda \in H(Q)^*$ satisfying this are exactly those in the lightly shaded regions. The elements in the darkly shaded region contains those $\lambda \in H^*(Q)$ for which $\sigma(\lambda) = 4$, meaning that the corresponding codewords $(f_\lambda(P_1), f_\lambda(P_2), \ldots, f_\lambda(P_n))$ are in $\tilde{E}(4)$, but not in $\tilde{E}(5)$.

15	19	23	27	31	35	39	43	47	51	55	59	63	67	71	75
10	14	18	22	26	30	34	38	42	46	50	54	58	62	66	70
5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65
0	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60

49	45	41	37	33	29	25	21	17	13	9	5	4	3	2	1
54	50	46	42	38	34	30	26	22	18	14	10	8	6	4	2
59	55	51	47	43	39	35	31	27	23	19	15	12	9	6	3
64	60	56	52	48	44	40	36	32	28	24	20	16	12	8	4

Figure 1. Graphical representation of the inclusions $\tilde{E}(5) \subsetneq \tilde{E}(4)$ over $\mathbb{F}_{16}$ from Example 3. Additional explanation may be found within the example.

4 Comparison with existing constructions

We will now compare the Steane-enlarged quantum codes from Section 3 to some of those already in the literature. In order to conserve space, the examples presented in this section will primarily be those where the constructions of the present paper improve upon existing constructions. This is not meant to imply that such improvements can always be expected – the cited works also contain specific examples of quantum codes whose parameters exceed what can be obtained using the results in Section 3.

For each code presented here, its parameters will also be compared to the Gilbert-Varshamov bound from [6].

Theorem 12. *Let $n > k \geq 2$ with $n \equiv k \pmod 2$, and let $d \geq 2$. Then there exists a pure stabilizer quantum code $[[n, k, d]]_q$ if the inequality*

$$\sum_{i=1}^{d-1} (q^2 - 1)^i \binom{n}{i} < q^{n-k+2} - 1 \tag{6}$$

is satisfied.

We will follow the same convention as [18] and write $[[n, k, d]]_q^{\ddagger}$ if the parameters (n, k, d) do not satisfy (6). That is, the $\ddagger$ indicates that the code parameters exceed those that are guaranteed by the Gilbert-Varshamov bound. If (6) instead holds for (n, k, d), but not for $(n, k, d + 1)$, we will denote the parameters of the code by $[[n, k, d]]_q^{\dagger}$. As stated in Theorem 12, these comparisons are only possible for $n \equiv k \pmod 2$. For code parameters (n, k, d) with $n \not\equiv k \pmod 2$ we shall use the same notation, but applied to $(n, k - 1, d)$. We note that [13; Cor. 4.3] is another Gilbert-Varshamov-type bound that allows $n \not\equiv k \pmod 2$, but for the codes presented in the following, Theorem 12 is stronger than [13; Cor. 4.3]. Therefore, only Theorem 12 will be used.

Example 4. *Comparing the codes found in Example 2 to Theorem 12, we obtain $[[64, 16, 20]]_{16}^{\ddagger}$ and $[[64, 14, 20]]_{16}^{\dagger}$. Thus, the Steane-enlarged code exceeds the Gilbert-Varshamov bound, whereas the CSS-code only meets the bound.*

Neither of the two codes presented in Example 3 meet or exceed the bound of Theorem 12.

In the two following examples, we will focus on comparison of quantum codes derived from the Hermitian function field. Specifically, we will compare the Steane-enlarged codes from Section 3 with the CSS-codes considered in [3].

Example 5. *For the order bound improved Hermitian codes from Section 3, we give in Table 1 a number of examples where the Steane-enlargement in Proposition 6 yields better parameters than those achievable in [3]. In all of these examples, the construction of [3] gives an asymmetric quantum code where $d_z - d_x = 1$. By using the Steane-enlargement technique, the minimal distance d_x can be increased by one, yielding a symmetric quantum code of*

the same dimension. That is, Steane-enlargement yields a code of parameters $[[n,k,d]]_{q^2}$*, where the construction of [3] yields* $[[n,k,d/(d-1)]]_{q^2}$*. Had we not applied Steane-enlargement in these cases, we would have to resort to the lower of the minimal distances when considering symmetric codes.*

All the codes given in Table 1 retain their original minimal distance during enlargement, and the columns marked Dim. increase *indicate the increase in dimension when applying Theorem 3 rather than Corollary 2.*

Example 6. *To exemplify the advantage of using the order bound improved codes and the Steane-enlargement technique, Table 2 shows a number of possible quantum code parameters over* $\mathbb{F}_{16}$ *when using different constructions based on the Hermitian function field. The codes in the first two columns stem from the CSS-construction applied to the usual one-point Hermitian codes, when bounding the distance by either the Goppa bound or the order bound. The third and fourth columns show the possible quantum code parameters when using order bound improved codes. In the third column, only the CSS-construction is used, and in the fourth Steane-enlargement is applied. Codes marked with* $*$ *have better parameters than all preceding codes in the same row.*

As is evident from the table, the use of the order bound gives more knowledge on the minimal distance in column two, but also provides even better parameters when applying Steane-enlargement to the order bound improved codes.

A different way to produce codes over $\mathbb{F}_9$ of length 27 is to consider codes from a Cartesian product of size $3 \cdot 9 = 27$, e.g. $\mathbb{F}_3 \times \mathbb{F}_9$, as described in [7]. In the next example, we consider two such Cartesian products and show

Code	Dim. increase
$[[8, 4, 3]]_4^{\ddagger}$	2
$[[27, 23, 3]]_9^{\ddagger}$	2
$[[27, 19, 4]]_9^{\dagger}$	2
$[[27, 11, 7]]_9^{\dagger}$	2
$[[64, 60, 3]]_{16}^{\ddagger}$	2
$[[64, 56, 4]]_{16}^{\dagger}$	2
$[[64, 51, 5]]_{16}$	3
$[[64, 40, 9]]_{16}^{\dagger}$	2
$[[64, 36, 10]]_{16}$	2
$[[64, 30, 13]]_{16}^{\dagger}$	2
$[[125, 121, 3]]_{25}^{\ddagger}$	2
$[[125, 117, 4]]_{25}^{\dagger}$	2
$[[125, 112, 5]]_{25}$	3
$[[125, 107, 6]]_{25}$	2
$[[125, 97, 9]]_{25}$	2
$[[125, 91, 11]]_{25}$	2
$[[125, 79, 16]]_{25}$	2
$[[125, 75, 17]]_{25}$	2

Code	Dim. increase
$[[125, 67, 21]]_{25}$	2
$[[343, 339, 3]]_{49}^{\ddagger}$	2
$[[343, 335, 4]]_{49}^{\ddagger}$	2
$[[343, 330, 5]]_{49}^{\dagger}$	3
$[[343, 325, 6]]_{49}$	2
$[[343, 319, 7]]_{49}$	4
$[[343, 313, 8]]_{49}$	2
$[[343, 308, 9]]_{49}$	3
$[[343, 289, 15]]_{49}$	2
$[[343, 284, 16]]_{49}$	3
$[[343, 271, 21]]_{49}$	2
$[[343, 267, 22]]_{49}$	2
$[[343, 258, 25]]_{49}$	3
$[[343, 251, 29]]_{49}$	2
$[[343, 244, 31]]_{49}$	3
$[[343, 235, 36]]_{49}$	2
$[[343, 231, 37]]_{49}$	2
$[[343, 219, 43]]_{49}$	2

Table 1. Comparison between nearly symmetric codes obtained via the procedure in Section 5 of [3] and the Steane enlarged codes from this paper. Further details are given in Example 5.

One-point codes		Order bound improved	
Goppa bound	**Order bound**	**CSS**	**Steane-enlargement**
$[[64, 30, 12]]_{16}$	$[[64, 30, 12]]_{16}$	$[[64, 30, 12]]_{16}$	$[[64, 30, 13]]^{\dagger}_{16}*$
$[[64, 32, 11]]_{16}$	$[[64, 32, 11]]_{16}$	$[[64, 32, 12]]^{\dagger}_{16}*$	$[[64, 32, 11]]_{16}$
$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$	$[[64, 34, 10]]_{16}$
$[[64, 36, 9]]_{16}$	$[[64, 36, 9]]_{16}$	$[[64, 36, 9]]_{16}$	$[[64, 36, 10]]_{16}*$
$[[64, 38, 8]]_{16}$	$[[64, 38, 9]]_{16}*$	$[[64, 38, 9]]_{16}$	$[[64, 38, 9]]_{16}$
$[[64, 39, 7]]_{16}$	$[[64, 39, 9]]_{16}*$	$[[64, 39, 6]]_{16}$	$[[64, 39, 9]]_{16}$
$[[64, 40, 7]]_{16}$	$[[64, 40, 8]]_{16}*$	$[[64, 40, 8]]_{16}$	$[[64, 40, 9]]^{\dagger}_{16}*$
$[[64, 42, 6]]_{16}$	$[[64, 42, 6]]_{16}$	$[[64, 42, 8]]_{16}*$	$[[64, 42, 7]]_{16}$
$[[64, 44, 5]]_{16}$	$[[64, 44, 5]]_{16}$	$[[64, 44, 6]]_{16}*$	$[[64, 44, 7]]_{16}*$
$[[64, 45, 4]]_{16}$	$[[64, 45, 5]]_{16}*$	$[[64, 45, 5]]_{16}$	$[[64, 45, 6]]_{16}*$
$[[64, 46, 4]]_{16}$	$[[64, 46, 5]]_{16}*$	$[[64, 46, 6]]_{16}*$	$[[64, 46, 5]]_{16}$
$[[64, 48, 3]]_{16}$	$[[64, 48, 5]]_{16}*$	$[[64, 48, 5]]_{16}$	$[[64, 48, 5]]_{16}$
$[[64, 50, 2]]_{16}$	$[[64, 50, 4]]_{16}*$	$[[64, 50, 4]]_{16}$	$[[64, 50, 5]]_{16}*$
$[[64, 51, 0]]_{16}$	$[[64, 51, 4]]_{16}*$	$[[64, 51, 4]]_{16}$	$[[64, 51, 5]]_{16}*$
$[[64, 54, 0]]_{16}$	$[[64, 54, 4]]_{16}*$	$[[64, 54, 4]]_{16}$	$[[64, 54, 3]]_{16}$
$[[64, 56, 0]]_{16}$	$[[64, 56, 3]]_{16}*$	$[[64, 56, 3]]_{16}$	$[[64, 56, 4]]^{\dagger}_{16}*$
$[[64, 58, 3]]^{\dagger}_{16}$	$[[64, 58, 3]]^{\dagger}_{16}*$	$[[64, 58, 3]]^{\dagger}_{16}$	$[[64, 58, 3]]^{\dagger}_{16}$
$[[64, 60, 0]]_{16}$	$[[64, 60, 2]]^{\dagger}_{16}*$	$[[64, 60, 2]]^{\dagger}_{16}$	$[[64, 60, 3]]^{\ddagger}_{16}*$
$[[64, 62, 0]]_{16}$	$[[64, 62, 2]]^{\dagger}_{16}*$	$[[64, 62, 2]]^{\dagger}_{16}$	$[[64, 62, 2]]^{\dagger}_{16}$

Table 2. Comparison between different methods for constructing quantum codes from the Hermitian function field over $\mathbb{F}_{16}$. Further details are given in Example 10.

how the resulting quantum code parameters compare against those of the Steane-enlarged codes from Section 3.

Example 7. *If we apply Theorem 3 to $\tilde{E}(7) \subsetneq \tilde{E}(6)$, we obtain a quantum code with parameters $[[27, 11, 7]]^{\dagger}_{9}$. Had we instead used the CSS-construction, Theorem 1, the best parameters would be $[[27, 9, 7]]^{\dagger}_{9}$ obtained from the code $\tilde{E}(7) = C_{\mathcal{L}}(D, 20Q)$. If we apply the CSS-construction to codes defined from the Cartesian product $\mathbb{F}_3 \times \mathbb{F}_9$, the best parameters with minimal distance 7 are $[[27, 5, 7]]_9$. By considering Steane-enlargement of codes from such Cartesian products as done in [4], the best parameters are instead $[[27, 8, 7]]_9$. Hence, the quantum code derived from Steane-enlargement of Hermitian codes improves the dimension significantly compared to the other three methods.*

Similar examples can be found over other fields. For instance, over $\mathbb{F}_{16}$ the Steane-enlargement of $\tilde{E}(9) \subsetneq \tilde{E}(8)$ produces parameters $[[64, 40, 9]]^{\dagger}_{16}$, whereas the CSS-construction applied to Hermitian codes yields $[[64, 38, 9]]_{16}$. The two Cartesian constructions give $[[64, 32, 9]]_{16}$ and $[[64, 35, 9]]_{16}$.

Instead of considering one-point algebraic geometric codes, it is also possible to consider the more general t-point codes in the hope of finding better parameters. The next example considers quantum codes from two- and three-point codes.

Example 8. *In [16], the authors give a general description of quantum codes that can be obtained by applying Theorem 1 to nested t-point algebraic geometric codes. They also give a number of corollaries [16; Cors. 3.3, 3.5, 3.6] that can readily be applied to the Hermitian function field to give specific parameters. For instance, [16; Table 2] contains the two-point Hermitian*

Two-Point Code	Three-Point Code	Section 3
$[[26, 16, 3]]_9$	$[[25, 15, 3]]_9$	$[[27, 23, 3]]_9^{\ddagger}$
$[[26, 14, 4]]_9$	$[[25, 13, 4]]_9$	$[[27, 19, 4]]_9^{\dagger}$
$[[26, 12, 5]]_9$	$[[25, 11, 5]]_9$	$[[27, 15, 5]]_9^{\dagger}$
$[[26, 4, 9]]_9^{\dagger}$	$[[25, 3, 9]]_9^{\dagger}$	$[[27, 5, 9]]_9^{\ddagger}$
$[[26, 2, 10]]_9^{\dagger}$	$[[25, 1, 10]]_9^{\dagger}$	$[[27, 3, 10]]_9^{\ddagger}$

Table 3. Examples of quantum codes from two- and three-point Hermitian codes over $\mathbb{F}_9$ from [16; Cor. 3.5] and [16; Cor. 3.6], respectively, along with the comparable codes from Section 3.

codes listed in the first column of Table 3. Turning to the three-point codes produced by [16; Cor. 3.6], the quantum codes with the same distances as the aforementioned two-point codes are given in the second column of Table 3. Finally, the third column shows the parameters produced by applying Theorem 3 to improved codes. The lengths of these are all one or two higher than the corresponding quantum code from the two-point and three-point Hermitian codes, respectively, but as evident from Table 3 the dimensions are significantly higher for small distances.

The last construction we will consider is La Guardia's construction of quantum generalized Reed-Solomon codes defined in [15]. These codes are asymmetric, but as mentioned in Section 2 they can be considered as symmetric by disregarding the highest of the two minimal distances.

Example 9. *Figure 2 shows the best possible dimension that can be obtained from three different methods given a desired minimal distance. The first method is the Steane-enlargement described in Section 3, and the second is the CSS-construction applied to Hermitian codes as in [3]. The final method comes from [15; Thm. 7.1] which yields quantum generalized Reed-Solomon codes. In this latter construction, codes of length q^3 over $\mathbb{F}_{q^2}$ are produced by choosing the defining parameters appropriately. But as noted in [7], better parameters can commonly be found by searching for codes of shorter length and then padding with zeros to obtain codes of length q^3. Thus, Figure 2 shows the best parameters when using this trick.*

As a final example, we will compare the codes from the current section to the quantum Singleton bound [14, 19].

Theorem 13. *Let $\mathcal{C}$ be a quantum code with parameters $[[n, k, d]]_q$, where $k > 0$. Then*

$$2d \leq n - k + 2.$$

Example 10. *A number of the codes presented in the preceding examples meet the quantum Singleton bound, Theorem 13. More precisely, this holds true for the code $[[27, 23, 3]]_9^{\ddagger}$ from Tables 1 and 3; the codes $[[64, 60, 3]]_{16}^{\ddagger}$, $[[125, 121, 3]]_{25}^{\ddagger}$, and $[[343, 339, 3]]_{49}^{\ddagger}$ from Table 1; and the codes $[[64, 62, 2]]_{16}^{\dagger}$ and $[[64, 60, 3]]_{16}^{\ddagger}$ from Table 2.*

5 Concluding remarks and acknowledgements

The results obtained in this work demonstrate that Steane-enlargement of improved Hermitian codes can produce quantum codes with significantly better parameters than other known constructions, especially for small designed distances. It is interesting whether similar, or better, parameters can be produced by the Steane-like technique from [8] when applied to such codes, but we leave this question open.

The authors wish to thank the anonymous reviewers for their thorough reading of the manuscript and their valuable suggestions.

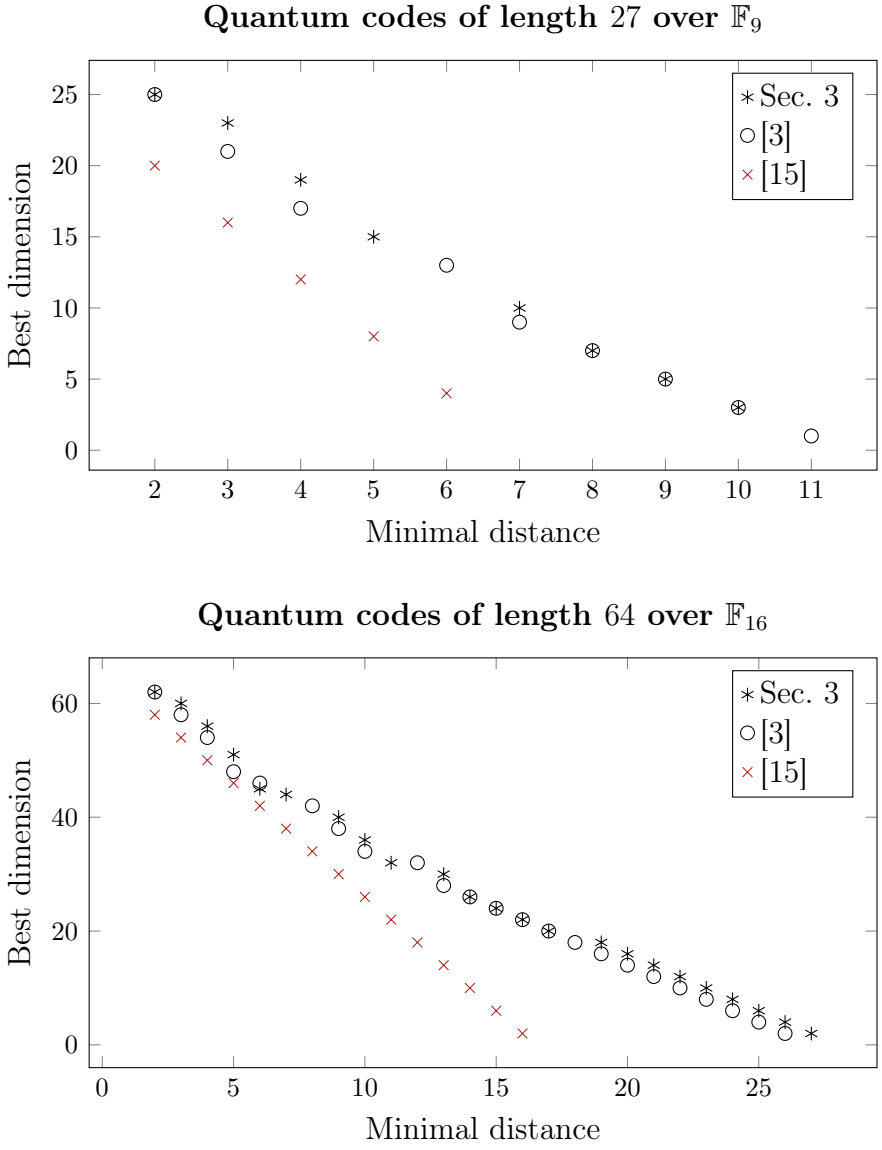

Figure 2. Plots showing the highest achievable dimension for a given minimal distance using the methods from Section 3, [3], and [15; Thm. 7.1].

References

[1] H. E. Andersen and O. Geil. "Evaluation codes from order domain theory". In: *Finite Fields Appl.* 14.1 (2008), pp. 92–123. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2006.12.004.

[2] A. R. Calderbank and P. W. Shor. "Good quantum error-correcting codes exist". In: *Phys. Rev. A* 54 (2 Aug. 1996), pp. 1098–1105. DOI: 10.1103/PhysRevA.54.1098.

[3] R. B. Christensen and O. Geil. "On nested code pairs from the Hermitian curve". In: *CoRR* abs/1807.04042 (2018). arXiv: 1807.04042. URL: http://arxiv.org/abs/1807.04042.

[4] R. B. Christensen and O. Geil. "On Steane-Enlargement of Quantum Codes from Cartesian Product Point Sets". In: *CoRR* abs/1908.04560 (2019). arXiv: 1908.04560. URL: http://arxiv.org/abs/1908.04560.

[5] I. M. Duursma and S. Park. "Coset bounds for algebraic geometric codes". In: *Finite Fields Appl.* 16.1 (2010), pp. 36–55. ISSN: 1071-5797. DOI: 10.1016/j.ffa.2009.11.006.

[6] K. Feng and Z. Ma. "A finite Gilbert-Varshamov bound for pure stabilizer quantum codes". In: *IEEE Trans. Information Theory* 50.12 (Dec. 2004), pp. 3323–3325. ISSN: 0018-9448. DOI: 10.1109/TIT.2004.838088.

[7] C. Galindo, O. Geil, F. Hernando and D. Ruano. "Improved Constructions of Nested Code Pairs". In: *IEEE Trans. Information Theory* 64.4 (2018), pp. 2444–2459. DOI: 10.1109/TIT.2017.2755682.

[8] C. Galindo, F. Hernando and D. Ruano. "Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement". In: *Quantum Inf. Process.* 14.9 (2015), pp. 3211–3231. DOI: 10.1007/s11128-015-1057-2.

[9] O. Geil. "On codes from norm-trace curves". In: *Finite Fields Appl.* 9.3 (2003), pp. 351–371. DOI: 10.1016/S1071-5797(03)00010-8.

[10] O. Geil, C. Munuera, D. Ruano and F. Torres. "On the order bounds for one-point AG codes". In: *Adv. Math. Commun.* 5.3 (2011), pp. 489–504. ISSN: 1930-5346. DOI: 10.3934/amc.2011.5.489.

[11] M. Hamada. "Concatenated Quantum Codes Constructible in Polynomial Time: Efficient Decoding and Error Correction". In: *IEEE Trans. Information Theory* 54.12 (Dec. 2008), pp. 5689–5704. ISSN: 0018-9448. DOI: 10.1109/TIT.2008.2006416.

[12] T. Høholdt, J. H. van Lint and R. Pellikaan. "Algebraic Geometry Codes". In: *Handbook of Coding Theory*. Ed. by V. S. Pless and W. C. Huffman. Vol. 1. Amsterdam: Elsevier, 1998, pp. 871–961.

[13] L. Jin and C. Xing. "Quantum Gilbert-Varshamov bound through symplectic self-orthogonal codes". In: *2011 IEEE International Symposium on Information Theory Proceedings*. July 2011, pp. 455–458. DOI: 10.1109/ISIT.2011.6034167.

[14] E. Knill and R. Laflamme. "Theory of quantum error-correcting codes". In: *Phys. Rev. A* 55 (2 Feb. 1997), pp. 900–911. DOI: 10.1103/PhysRevA.55.900.

[15] G. G. La Guardia. "Asymmetric quantum Reed-Solomon and generalized Reed-Solomon codes". In: *Quantum Inf. Process.* 11.2 (Apr. 2012), pp. 591–604. ISSN: 1573-1332. DOI: 10.1007/s11128-011-0269-3.

[16] G. G. La Guardia and F. R. F. Pereira. "Good and asymptotically good quantum codes derived from algebraic geometry". In: *Quantum Inf. Process.* 16.6 (May 2017), p. 165. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1618-7.

[17] S. Ling, J. Luo and C. Xing. "Generalization of Steane's enlargement construction of quantum codes and applications". In: *IEEE Trans. Information Theory* 56.8 (2010), pp. 4080–4084. DOI: 10.1109/TIT.2010.2050828.

[18] C. Munuera, W. Tenório and F. Torres. "Quantum error-correcting codes from algebraic geometry codes of Castle type". In: *Quantum Inf. Process.* 15.10 (Oct. 2016), pp. 4071–4088. ISSN: 1573-1332. DOI: 10.1007/s11128-016-1378-9.

[19] E. M. Rains. "Nonbinary quantum codes". In: *IEEE Trans. Information Theory* 45.6 (Sept. 1999), pp. 1827–1832. ISSN: 0018-9448. DOI: 10.1109/18.782103.

[20] P. K. Sarvepalli, A. Klappenecker and M. Rötteler. "Asymmetric quantum codes: constructions, bounds and performance". In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 465 (2009), pp. 1645–1672. DOI: 10.1098/rspa.2008.0439.

[21] P. K. Sarvepalli and A. Klappenecker. "Nonbinary Quantum Codes from Hermitian Curves". In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Ed. by M. P. C. Fossorier, H. Imai, S. Lin and A. Poli. Springer Berlin Heidelberg, 2006, pp. 136–143. ISBN: 978-3-540-31424-0. DOI: 10.1007/11617983_13.

[22] A. Steane. "Multiple-Particle Interference and Quantum Error Correction". In: *Proc. R. Soc. Lond. Ser. A: Math. Phys. Eng. Sci.* 452.1954 (1996), pp. 2551–2577. ISSN: 13645021.

[23] A. M. Steane. "Enlargement of Calderbank-Shor-Steane quantum codes". In: *IEEE Trans. Information Theory* 45.7 (1999), pp. 2492–2495. DOI: 10.1109/18.796388.

[24] H. Stichtenoth. *Algebraic Function Fields and Codes*. 2nd ed. Graduate Texts in Mathematics. Springer, 2009. ISBN: 978-3-540-76877-7.

[25] H. Tiersma. "Remarks on codes from Hermitian curves". In: *IEEE Trans. Information Theory* 33.4 (July 1987), pp. 605–609. ISSN: 0018-9448. DOI: 10.1109/TIT.1987.1057327.

[26] K. Yang and P. V. Kumar. "On the true minimum distance of Hermitian codes". In: *Coding theory and algebraic geometry*. Ed. by H. Stichtenoth and M. A. Tsfasman. Springer, 1992, pp. 99–107.